Кібератака групи UAC-0026 з використанням шкідливої програми HeaderTip (CERT-UA#4244)

Загальна інформація

Урядовою командою реагування на комп’ютерні надзвичайні події України CERT-UA виявлено RAR-архів "Про збереження відеоматеріалів з фіксацією злочинних дій армії російської федерації.rar", який містить одноіменний EXE-файл. Запуск виконуваного файлу призведе до створення на комп'ютері документу-приманки "#2163_02_33-2022.pdf" (стосується листа Національної поліції України), а також DLL-файлу з видаленим MZ-заголовком "officecleaner.dat" та BAT-файлу "officecleaner.bat", що забезпечить формування коректного DLL-файлу, його запуск і запис в реєстр Windows для забезпечення персистентності.

Згаданий DLL-файл класифіковано як шкідливу програму HeaderTip, основним призначенням якої є завантаження та виконання інших DLL-файлів.

Активність відстежується за ідентифікатором UAC-0026. Аналогічні атаки, для прикладу, фіксувалися у вересні 2020 року.

Індикатори компрометації

Файли:

```
1af894a5f23713b557c23078809ed01c
839e968aa5a6691929b4d65a539c2261f4ecd1c504a8ba52abbfbac0774d6fa3    Про збереження відеоматеріалів з фіксацією злочинних дій армії російської федерації.rar
13612c99a38b2b07575688c9758b72cc
042271aadf2191749876fc99997d0e6bdd3b89159e7ab8cd11a9f13ae65fa6b1    Про збереження відеоматеріалів з фіксацією злочинних дій армії російської федерації.exe
3293ba0e2eaefbe5a7c3d26d0752326e
c0962437a293b1e1c2702b98d935e929456ab841193da8b257bd4ab891bf9f69
#2163_02_33-2022.pdf (документ-приманка)
9c22548f843221cc35de96d475148ecf
830c6ead1d972f0f41362f89a50f41d869e8c22ea95804003d2811c3a09c3160
officecleaner.bat
4fb630f9c5422271bdd4deb94a1e74f4
a2ffd62a500abbd157e46f4caeb91217738297709362ca2c23b0c2d117c7df38
officecleaner.dat
```

```
1aba36f72685c12e60fb0922b606417c
63a218d3fc7c2f7fcadc0f6f907f326cc86eb3f8cf122704597454c34c141cf1
httpshelper.dll (HeaderTip)
```

Мережеві:

```
Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
hxxps://product2020.mrbasic[.]com:8080
product2020.mrbasic[.]com
104[.]155.198.25
```

Хостові:

```
%TMP%\#2163_02_33-2022.pdf
%TMP%\officecleaner.bat
%TMP%\officecleaner.dat
%TMP%\officecleaner.dll
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\httpsrvlog
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\httpshelper
c:\windows\system32\rundll32.exe %TMP%\httpshelper.dll,OAService
```

Графічні зображення

НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ

вул. Богомольця, 10, м. Київ, 01601,
тел. 254-93-33, info@police.gov.ua

Ідентифікаційний код 40108578

16.03.2022 року №

На № від

Заступникам начальників – начальникам кримінальної поліції головних управлінь Національної поліції в областях та м. Києві

Про збереження відеоматеріалів з фіксацією злочинних дій армії російської федерації

24 лютого росія розпочала відкрите військове вторгнення до України, у тому числі з території Республіки Білорусь. Вже декілька тижнів відбуваються ракетні обстріли військової та цивільної інфраструктури по всій країні, гинуть мирні жителі, знищується майно та відбувається системне вчинення військових та злочинів проти людства військовослужбовцями армії росії.

В умовах військового стану та знищення, у тому числі об'єктів та ресурсів органів і підрозділів Національної поліції України, існує потреба у максимальному збереженні всіх доступних відеоматеріалів на яких фіксується вчинення різних злочинів армією росії.

Зокрема до таких відеоматеріалів слід віднести відеозаписи із загальнообласних та міських систем відеонагляду (Безпечне місто, Безпечний регіон), а також інших відеокамер будь-якої форми власності щодо переміщення (руху) ворожої техніки, моментів обстрілів та бомбардування, нанесення артилерійських чи авіаційних ударів по житлових будинках, школах, дитсадках, лікарнях, електростанціях та інших об'єктах забезпечення життєдіяльності населених пунктів, обстріли колон евакуації цивільних осіб, випадки вчинення мародерства та інших диверсійно-розвідувальних, протиправних і злочинних діянь. Крім того, слід приділити увагу щодо збереження відеозаписів розміщених у різних групах «месенджерів», ресурсах мережі інтернет та відео-сюжетів зроблених очевидцями таких подій (записи на телефонах та відео реєстраторах).

З огляду на викладене прошу розглянути питання щодо забезпечення збереження зазначених вище видів відеоматеріалів, та за можливості їх резервних копій, з метою подальшого долучення до матеріалів досудового розслідування та використання під час аналітичних досліджень працівниками підрозділів кримінального аналізу.